BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 62, No. 3, 2014

COMMUTATIVE ALGEBRA

Relations between Elements $r^{p^l} - r$ and $p \cdot 1$ for a Prime p

by

Andrzej PRÓSZYŃSKI

Presented by Andrzej SCHINZEL

Summary. For any positive power n of a prime p we find a complete set of generating relations between the elements $[r] = r^n - r$ and $p \cdot 1$ of a unitary commutative ring.

1. Introduction. Let R be a commutative ring with 1. In [2], the author introduced the ideals $I_n(R)$ generated by all elements $r^n - r$ where $r \in R$. It follows from [2, Proposition 5.5] that $I_n(R)$ is precisely the intersection of all maximal ideals M of R such that $|R/M| - 1$ divides $n - 1$. The main result of [1] determines generating relations for the generators $r^n - r$ of $I_n(R)$, where n is a power of 2 or $n = 3$ (Theorem 1).

In [3], the author introduced the ideals $I'_p(R) = I_p(R) + pR$ for prime p. It follows from [3, Theorem 1.4.8] that $I'_p(R)$ is precisely the intersection of all maximal ideals M of R such that $|R/M| = p$. In this paper, we consider the more general case of ideals $I'_n(R) = I_n(R) + pR$, generated by all elements $r^n - r$ for $r \in R$ and the element $p \cdot 1 \in R$, where $n = p^l$ for $l = 1, 2, \ldots$. The purpose of this paper is to find a complete set of generating relations between these elements (Theorem 1), generalizing also (in Corollary 4) a part of [1, Theorem 1].

2. n-derivations. Recall some ideas of [1]. If f is a mapping between R-modules and $f(0) = 0$ then we define

$$(\Delta^2 f)(x, y) = f(x + y) - f(x) - f(y).$$

Let n be a fixed natural number. By an *n-derivation* over R we mean a function $f\colon R \longrightarrow M$, where M is an R-module, satisfying the following

2010 *Mathematics Subject Classification*: 13C13, 13C05, 11E76.
Key words and phrases: ideals of commutative rings, generators and relations, higher degree mappings.

DOI: 10.4064/ba62-3-4

condition:

$$(\mathrm{D}_n) \qquad f(rs) = r^n f(s) + s f(r), \qquad r, s \in R.$$

For example, the function $f\colon R \to R$, $f(r) = r^n - r$, is an n-derivation. On the other hand, any (ordinary) derivation is a 1-derivation.

The following lemma contains some new properties.

LEMMA 1. *If f is an n-derivation then for any $r, s \in R$ we have*

(1) $(r^n - r)f(s) = (s^n - s)f(r)$,
(2) $f(0) = f(1) = 0$,
(3) *if s is invertible then* $f(s^{-1}) = -s^{-n-1}f(s)$,
(4) $f(r^k) = (r^{n(k-1)} + r^{n(k-2)+1} + r^{n(k-3)+2} + \cdots + r^{n+(k-2)} + r^{k-1})f(r)$,
(5) *if n is a positive power of a prime p and p divides k then $f(r^k) = af(r)$ where $a \in I'_n(R)$.*

Proof. Relation (1) follows from the two symmetric versions of (D_n). The equalities $f(0) = f(1) = 0$ follow from (D_n) for $r = s = 0$ or 1. Using (D_n) and (2) we obtain $0 = f(1) = f(s \cdot s^{-1}) = s^n f(s^{-1}) + s^{-1} f(s)$, and this gives (3). Property (4) follows from (D_n) by induction.

(5) Since $r^n \equiv r \bmod I'_n(R)$, the coefficient in (4) is congruent to kr^{k-1}. This belongs to $I'_n(R)$ since $p \mid k$ and $p \cdot 1 \in I'_n(R)$. ∎

Let S be a multiplicatively closed set in R.

PROPOSITION 1. *For any n-derivation $f\colon R \to M$ there exists a unique n-derivation $f_S\colon R_S \to M_S$ satisfying the condition $f_S(i(r)) = i(f(r))$ for $r \in R$. It is given by the formula*

$$f_S\left(\frac{r}{s}\right) = \frac{f(r)}{s} - \left(\frac{r}{s}\right)^n \frac{f(s)}{s} = \frac{sf(r) - rf(s)}{s^{n+1}}.$$

Moreover,

$$(\Delta^2 f_S)\left(\frac{r}{t}, \frac{s}{t}\right) = \frac{(\Delta^2 f)(r, s)}{t^n}.$$

3. C'-functions. Let p be a fixed prime and n a fixed natural number of the form $n = p^l$, $l = 1, 2, \ldots$. Let M be an R-module with a fixed element $m_0 \in M$. We will call an n-derivation $f\colon R \to M$ *semi-additive*, and denote $f\colon R \to (M, m_0)$, if it satisfies the additional condition

$$(\mathrm{C}'_n) \qquad f(r+s) = f(r) + f(s) + N(r,s)m_0, \qquad r, s \in R,$$

or equivalently

$$(\mathrm{C}''_n) \qquad (\Delta^2 f)(r, s) = N(r,s)m_0, \qquad r, s \in R,$$

where

$$N(r,s) = \sum_{k=1}^{n-1} \frac{1}{p} \binom{n}{k} r^{n-k} s^k$$

(note that $\frac{1}{p}\binom{n}{k} \in \mathbb{Z}$ for $k = 1, \dots, n-1$ because of the shape of n). Using the generalized Newton symbols

$$\begin{aligned}(i_1, \dots, i_k) &= \frac{(i_1 + \dots + i_k)!}{i_1! \dots i_k!} \\ &= \binom{i_1 + \dots + i_k}{i_k} \binom{i_1 + \dots + i_{k-1}}{i_{k-1}} \dots \binom{i_1 + i_2}{i_2} \\ &= (i_1 + \dots + i_{k-1}, i_k)(i_1, \dots, i_{k-1})\end{aligned}$$

we define the following generalization of $N(r,s)$:

$$N(r_1, \dots, r_k) = \sum \frac{1}{p} (i_1, \dots, i_k) r_1^{i_1} \dots r_k^{i_k},$$

where the sum is over all systems of non-negative integers $i_1, \dots, i_k$ such that $i_1 + \dots + i_k = n$ and at least two i_j are non-zero (then all the coefficients in the sum are integers). In particular, for any integers $m_1, \dots, m_k$, the generalized Newton formula shows that

$$N(m_1 \cdot 1, \dots, m_k \cdot 1) = \frac{1}{p}((m_1 + \dots + m_k)^n - m_1^n - \dots - m_k^n) \cdot 1,$$

and for $m_1 = \dots = m_k = 1$ we get $N(1, \dots, 1) = \frac{1}{p}(k^n - k) \cdot 1$.

Lemma 2. *For any $r_1, \dots, r_k, r_{k+1} \in R$ we have*

(1) $N(r_1, \dots, r_k, r_{k+1}) = N(r_1 + \dots + r_k, r_{k+1}) + N(r_1, \dots, r_k)$,

(2) $f\Big(\sum_{i=1}^{k} r_i\Big) = \sum_{i=1}^{k} f(r_i) + N(r_1, \dots, r_k) m_0$

provided that f satisfies (C'_n).

Proof. (1) The generalized Newton formula shows that

$$\begin{aligned}N(r_1 + \dots + r_k, r_{k+1}) &= \sum_{\substack{j_1 + j_2 = n \\ j_1, j_2 > 0}} \frac{1}{p} (j_1, j_2)(r_1 + \dots + r_k)^{j_1} r_{k+1}^{j_2} \\ &= \sum_{\substack{j_1 + j_2 = n \\ j_1, j_2 > 0}} \sum_{i_1 + \dots + i_k = j_1} \frac{1}{p} (j_1, j_2)(i_1, \dots, i_k)(r_1^{i_1} \dots r_k^{i_k}) r_{k+1}^{j_2}\end{aligned}$$

$$= \sum_{\substack{i_1+\dots+i_{k+1}=n \\ i_1+\dots+i_k>0,\, i_{k+1}>0}} \frac{1}{p}(i_1+\dots+i_k, i_{k+1})(i_1,\dots,i_k) r_1^{i_1}\dots r_k^{i_k} r_{k+1}^{i_{k+1}}$$

$$= \sum_{\substack{i_1+\dots+i_{k+1}=n \\ i_1+\dots+i_k>0,\, i_{k+1}>0}} \frac{1}{p}(i_1,\dots,i_k,i_{k+1}) r_1^{i_1}\dots r_{k+1}^{i_{k+1}}.$$

Since $(i_1,\dots,i_k,0) = (i_1,\dots,i_k)$, the above is equal to $N(r_1,\dots,r_k,r_{k+1}) - N(r_1,\dots,r_k)$, as required.

(2) For $k=2$ see (C'_n). If (2) holds for some $k \ge 2$ then, by (C'_n) and (1),

$$\begin{aligned} f\Big(\sum_{i=1}^{k+1} r_i\Big) &= f\Big(\sum_{i=1}^{k} r_i\Big) + f(r_{k+1}) + N\Big(\sum_{i=1}^{k} r_i, r_{k+1}\Big)m_0 \\ &= \sum_{i=1}^{k} f(r_i) + N(r_1,\dots,r_k)m_0 + f(r_{k+1}) + N(r_1+\dots+r_k, r_{k+1})m_0 \\ &= \sum_{i=1}^{k+1} f(r_i) + N(r_1,\dots,r_{k+1})m_0. \ \blacksquare \end{aligned}$$

COROLLARY 1. *Let $f\colon R \to (M, m_0)$ be a semi-additive n-derivation. Then*

(1) $f(pr) = pf(r) + (p^{n-1}-1)r^n m_0$,
(2) $f(p\cdot 1) = (p^{n-1}-1)m_0$.

If $p^{n-1}-1$ is invertible in R and $u = (p^{n-1}-1)^{-1} \in R$ then

(3) $m_0 = uf(p\cdot 1)$,
(4) $pf(r) = (r^n - r)m_0$.

Proof. Setting $k = p$ and $r_i = r$ in Lemma 2(2) we obtain (1), since $N(1,\dots,1) = \frac{1}{p}(p^n - p)\cdot 1$. Then Lemma 1(2) gives (2) and (3). It follows from Lemma 1(1) and from (2) above that

$$(p^n - p)f(r) = (r^n - r)f(p\cdot 1) = (r^n - r)(p^{n-1}-1)m_0.$$

Then multiplication by u gives (4). ■

By a *C'-function of degree n over R* we will mean a semi-additive n-derivation $f\colon R \to (M, m_0)$ satisfying condition (4) of the above lemma. In other words, it is assumed that the following conditions are fulfilled:

(D_n)	$f(rs) = r^n f(s) + sf(r)$,	$r, s \in R$,
(C'_n)	$f(r+s) = f(r) + f(s) + N(r,s)m_0$,	$r, s \in R$,
(E_n)	$pf(r) = (r^n - r)m_0$,	$r \in R$.

EXAMPLE 1. The function $f\colon R \to (R, p \cdot 1)$, $f(r) = r^n - r$, is a C'-function of degree n. Indeed, it is an n-derivation, (C'_n) is satisfied since

$$(r+s)^n - (r+s) - (r^n - r) - (s^n - s) = \sum_{k=0}^{n} \binom{n}{k} r^{n-k} s^k - r^n - s^n$$
$$= p \sum_{k=1}^{n-1} \frac{1}{p} \binom{n}{k} r^{n-k} s^k = N(r,s)(p \cdot 1)$$

by the Newton binomial formula, and (E_n) is obvious. Later, we prove that it is a universal C'-function of degree n (Theorem 1).

EXAMPLE 2. A C'-function of degree 3 is a 3-derivation $f\colon R \to (M, m_0)$ such that $3f(r) = (r^3 - r)m_0$ and $f(r+s) = f(r) + f(s) + (r^2 s + rs^2)m_0$ for $r, s \in R$. Then $f(2) = 2m_0$ and it is easy to check that f satisfies conditions (C1)–(C3) of [1], showing that f is a so called C-function of degree 3.

EXAMPLE 3. Let R be the polynomial ring $\mathbb{Z}_2[X]$, $M = \mathbb{Z}_2 = \mathbb{Z}_2[X]/(X)$ and $m_0 = 1 + (X)$. Then for any $g = \sum_i g_i X^i \in \mathbb{Z}_2[X]$, $m \in M$ and $k = 1, 2, \ldots$ we have $g^k m = g_0^k m = g_0 m$. Define $f\colon \mathbb{Z}_2[X] \to M$ by $f(g) = g_1 + (X)$. Since

$$f(gh) = g_0 h_1 + h_0 g_1 + (X) = g^n f(h) + h f(g)$$

it follows that f is an n-derivation for any n. Let now n be a power of an odd prime p. Then $N(g,h)m_0 = N(g_0, h_0)m_0 = 0$ for any $g, h \in \mathbb{Z}_2[X]$ since $N(1,1) = \frac{1}{p}(2^n - 2)$ is even. Moreover, f is additive, and hence it is semi-additive (actually, it is the only semi-additive n-derivation $f\colon \mathbb{Z}_2[X] \to (M, m_0)$ satisfying $f(X) = 1 + (X)$). On the other hand, (E_n) is not fulfilled, since $pf(X) = 1 + (X) \neq 0$ and $(X^n - X)m_0 = 0$. Hence f is not a C'-function of degree n.

4. The functors $C' = C'^{(n)}$. Let $n = p^l$, $l = 1, 2, \ldots$ Denote by $C'(R) = C'^{(n)}(R)$ the R-module generated by elements denoted by $[r]$, $r \in R$, and an extra element $[*]$, with the following relations:

(D) $\qquad [rs] = r^n[s] + s[r], \qquad r, s \in R,$

(C′) $\qquad [r+s] = [r] + [s] + N(r,s)[*], \qquad r, s \in R,$

(E) $\qquad p[r] = (r^n - r)[*], \qquad r \in R.$

Any unitary ring homomorphism $i\colon R \to R'$ induces a module homomorphism $C'(i)\colon C'(R) \to C'(R')$ over i such that $C'(i)([r]) = [i(r)]$ and $C'(i)([*]) = [*]$. This shows that C' is a functor to the category of modules (over all commutative rings) with fixed elements. Observe that $C'(R)$ is a universal object with respect to C'-functions of degree n over R, meaning that any C'-function of degree n can be uniquely expressed as the composition of the canonical C'-function $c'\colon R \to (C'(R), [*]), c'(r) = [r]$, and an R-homomorphism defined on $C'(R)$ and preserving the fixed elements.

In particular, the C'-function $f\colon R \to (R, p \cdot 1)$, $f(r) = r^n - r$, gives

Corollary 2. *There exists an R-homomorphism $P\colon C'(R) \to I'_n(R)$ such that $P([r]) = r^n - r$ for $r \in R$ and $P([*]) = p \cdot 1$.*

Our goal is to show that P is an isomorphism (Theorem 1). As a first step, we prove that C' commutes with localizations. Let S be a multiplicatively closed set in R and let $i\colon R \to R_S$ and $i\colon M \to M_S$ be the canonical homomorphisms, $i(r) = \frac{r}{1}$, $i(m) = \frac{m}{1}$.

Proposition 2. *If $f\colon R \to (M, m_0)$ is a C'-function of degree n (or a semi-additive n-derivation) then so is the function*

$$f_S\colon R_S \to \left(M_S, \frac{m_0}{1}\right), \qquad f_S(i(r)) = i(f(r)),$$

defined in Proposition 1.

Proof. Using Proposition 1 we compute that

$$(\mathrm{C}''_n)\quad (\Delta^2 f_S)\left(\frac{a}{s}, \frac{b}{s}\right) = \frac{(\Delta^2 f)(a,b)}{s^n} = \frac{N(a,b)m_0}{s^n} = N\left(\frac{a}{s}, \frac{b}{s}\right)\frac{m_0}{1},$$

$$(\mathrm{E}_n)\qquad pf_S\left(\frac{r}{s}\right) = \frac{s(p(f(r)) - r(pf(s))}{s^{n+1}} = \frac{s(r^n - r)m_0 - r(s^n - s)m_0}{s^{n+1}} = \left(\left(\frac{r}{s}\right)^n - \frac{r}{s}\right)\frac{m_0}{1}. \ \blacksquare$$

Proposition 3. *There exists an R_S-isomorphism $C'(R)_S \approx C'(R_S)$ such that*

$$\frac{[r]}{s} \leftrightarrow \frac{1}{s}\left[\frac{r}{1}\right], \qquad \frac{[*]}{1} \leftrightarrow [*].$$

Proof. Proposition 2 applied to the canonical C'-function $c'\colon R \to (C'(R), [*]), c'(r) = [r]$, gives an C'-function $c'_S\colon R_S \to \left(C'(R)_S, \frac{[*]}{1}\right)$ over R_S, where

$$c'_S\left(\frac{r}{s}\right) = \frac{[r]}{s} - \left(\frac{r}{s}\right)^n \frac{[s]}{s}.$$

The universal property yields an R_S-homomorphism $g\colon C'(R_S) \to C'(R)_S$ such that

$$g\left(\left[\frac{r}{s}\right]\right) = c'_S\left(\frac{r}{s}\right) = \frac{[r]}{s} - \left(\frac{r}{s}\right)^n \frac{[s]}{s}, \qquad g([*]) = \frac{[*]}{1}.$$

On the other hand, the homomorphism $C'(i)\colon C'(R) \to C'(R_S)$ over $i\colon R\to R_S$, defined by $C'(i)([r]) = \left[\frac{r}{1}\right]$, $C'(i)([*]) = [*]$, gives an R_S-homomorphism

$$h\colon C'(R)_S \to C'(R_S), \qquad h\left(\frac{[r]}{s}\right) = \frac{1}{s}\left[\frac{r}{1}\right], \qquad h\left(\frac{[*]}{1}\right) = [*].$$

Observe that $h = g^{-1}$. Indeed,

$$g\left(h\left(\frac{[r]}{s}\right)\right) = \frac{1}{s} g\left(\left[\frac{r}{1}\right]\right) = \frac{1}{s}\left(\frac{[r]}{1} - \left(\frac{r}{1}\right)^n \frac{[1]}{1}\right) = \frac{[r]}{s}$$

by Lemma 1(2). On the other hand, using Lemma 1(3) and (D) we compute that

$$\begin{aligned} h\left(g\left(\left[\frac{r}{s}\right]\right)\right) &= h\left(\frac{[r]}{s} - \left(\frac{r}{s}\right)^n \frac{[s]}{s}\right) = \frac{1}{s}\left[\frac{r}{1}\right] - \frac{r^n}{s^{n+1}}\left[\frac{s}{1}\right] \\ &= \frac{1}{s}\left[\frac{r}{1}\right] + \left(\frac{r}{1}\right)^n \left[\frac{1}{s}\right] = \left[\frac{r}{1}\frac{1}{s}\right] = \left[\frac{r}{s}\right]. \end{aligned}$$

Hence h is an isomorphism, as required. ∎

5. The main lemmas. We consider the kernel of the R-epimorphism $P\colon C'(R) \to I'_n(R)$, $P([r]) = r^n - r$ for $r\in R$ and $P([*]) = p\cdot 1$.

Lemma 3.

(1) $P(x)y = P(y)x$ *for any* $x, y \in C'(R)$,
(2) $I'_n(R)\operatorname{Ker}(P) = 0$.

Proof. (1) For $x = [r],\ y = [s]$ apply Lemma 1(1), and for $x = [r],\ y = [*]$ apply (E).

(2) If $r \in I'_n(R)$ and $y \in \operatorname{Ker}(P)$ then $r = P(x)$ and hence $ry = P(x)y = P(y)x = 0$ by (1). ∎

Let now $p^{n-1} - 1$ be invertible in R. Hence $[*] = u[p\cdot 1]$ (Corollary 2) and Lemma 2(2) gives the following formula:

$$(*)\quad \left[\sum_{i=1}^k r_i\right] = \sum_{i=1}^k [r_i] + N(r_1,\ldots,r_k)[*] = \sum_{i=1}^k [r_i] + N(r_1,\ldots,r_k)u[p\cdot 1].$$

Moreover, any element of $C'(R)$ is of the form $\sum_i a_i[r_i]$, where $a_i, r_i \in R$.

Lemma 4. *Let* $p^{n-1} - 1$ *be invertible in* R *and* $x = \sum_{i=1}^k a_i[r_i] \in \operatorname{Ker}(P)$, *where one of the* r_i *is* $p\cdot 1$. *If all* a_i *belong to* $I'_n(R)^m$ *for some* $m \geq 0$ *then* $x = \sum_{i=1}^k b_i[r_i]$ *where all* b_i *belong to* $I'_n(R)^{nm+1}$.

Proof. By the assumption $\sum_{i=1}^k a_i r_i^n = \sum_{i=1}^k a_i r_i$. Using $(*)$ we obtain

$$\Big[\sum_{i=1}^k a_i r_i\Big] = \sum_{i=1}^k [a_i r_i] + N_1 u[p\cdot 1] = \sum_{i=1}^k a_i[r_i] + \sum_{i=1}^k r_i^n[a_i] + N_1 u[p\cdot 1],$$

$$\Big[\sum_{i=1}^k a_i r_i^n\Big] = \sum_{i=1}^k [a_i r_i^n] + N_2 u[p\cdot 1] = \sum_{i=1}^k a_i^n[r_i^n] + \sum_{i=1}^k r_i^n[a_i] + N_2 u[p\cdot 1],$$

where

$$N_1 = N(a_1r_1,\ldots,a_kr_k) = \sum \frac{1}{p}(i_1,\ldots,i_k)a_1^{i_1}\ldots a_k^{i_k} r_1^{i_1}\ldots r_k^{i_k},$$

$$N_2 = N(a_1r_1^n,\ldots,a_kr_k^n) = \sum \frac{1}{p}(i_1,\ldots,i_k)a_1^{i_1}\ldots a_k^{i_k} (r_1^{i_1}\ldots r_k^{i_k})^n,$$

and the sums are over all systems of non-negative integers $i_1,\ldots,i_k$ such that $i_1+\cdots+i_k = n$ and at least two i_j are non-zero. Since

$$\sum_{i=1}^k a_i[r_i] + \sum_{i=1}^k r_i^n[a_i] + N_1 u[p\cdot 1] = \sum_{i=1}^k a_i^n[r_i^n] + \sum_{i=1}^k r_i^n[a_i] + N_2 u[p\cdot 1]$$

we obtain

$$\begin{aligned} x = \sum_{i=1}^k a_i[r_i] &= \sum_{i} a_i^n[r_i^n] + (N_2-N_1)u[p\cdot 1] \\ &= \sum_{i=1}^k a_i^n a[r_i] + (N_2-N_1)u[p\cdot 1], \end{aligned}$$

where $a\in I_n'(R)$ by Lemma 1(5). Since $a_i \in I_n'(R)^m$ it follows that $a_i^n a \in I_n'(R)^{nm+1}$.

Moreover, $a_1^{i_1}\ldots a_k^{i_k} \in I_n'(R)^{nm}$ since $a_i\in I_n'(R)^m$ and $i_1+\cdots+i_k = n$, and $(r_1^{i_1}\ldots r_k^{i_k})^n - r_1^{i_1}\ldots r_k^{i_k} \in I_n'(R)$. Hence

$$N_2 - N_1 = \sum \frac{1}{p}(i_1,\ldots,i_k)a_1^{i_1}\ldots a_k^{i_k}\big((r_1^{i_1}\ldots r_k^{i_k})^n - r_1^{i_1}\ldots r_k^{i_k}\big) \in I_n'(R)^{nm+1}.$$

This completes the proof. ∎

The above lemma immediately gives

Corollary 3. *Let $p^{n-1}-1$ be invertible in R and $x = \sum_{i=1}^k a_i[r_i]$ be an arbitrary element of* $\mathrm{Ker}(P)$. *Let M denote the submodule of $C'(R)$ generated by $[r_1],\ldots,[r_k]$ and $[p\cdot 1]$ (or $[*]$). Then*

$$x \in \bigcap_{m=0}^{\infty} I_n(R)^m M.$$

6. The main theorem. The purpose of this paper is to prove the following.

THEOREM 1. *Let $C'(R) = C'^{(n)}(R)$ where $n = p^l$, $l = 1, 2, \ldots$. Then $P\colon C'(R) \to I'_n(R)$, $P([r]) = r^n - r$ for $r \in R$ and $P([*]) = p \cdot 1$, is an R-isomorphism. In other words, if $n = p^l$, $l = 1, 2, \ldots$, then the following are generating relations between the generators $[r] = r^n - r$ and $[*] = p \cdot 1$ of $I'_n(R)$:*

(D) $$[rs] = r^n[s] + s[r], \qquad r, s \in R,$$

(C′) $$[r + s] = [r] + [s] + N(r, s)[*], \qquad r, s \in R,$$

where $N(r, s) = \sum_{k=1}^{n-1} \frac{1}{p}\binom{n}{k} r^{n-k} s^k$, and

(E) $$p[r] = (r^n - r)[*], \qquad r \in R.$$

Proof. Our goal is to prove that $\mathrm{Ker}(P) = 0$.

Noetherian case. Assume that R is noetherian. By Proposition 3 we can assume that R is local and noetherian with quotient field K. Then $I_n(R)$ is the maximal ideal if $|K| - 1$ divides $n - 1$, and $I_n(R) = R$ otherwise (see Introduction). Hence $I'_n(R)$ is the maximal ideal if $|K| - 1$ divides $n - 1$ and $\mathrm{char}(K) = p$, and $I'_n(R) = R$ otherwise. If $I'_n(R) = R$ then Lemma 3 shows that $\mathrm{Ker}(P) = 0$, as desired. So let $I'_n(R)$ be the maximal ideal of R.

Since $p \in I'_n(R)$, $p^{n-1} - 1$ is invertible in R. Let $x \in \mathrm{Ker}(P)$. Define the submodule M as in Corollary 3 and observe that it is finitely generated over a local noetherian ring. Then the intersection in the corollary is zero by the Krull intersection theorem, and hence $x = 0$. This proves that $\mathrm{Ker}(P) = 0$.

General case. Let $x = \sum_i a_i[r_i] + a_0[*] \in \mathrm{Ker}(P)$. Define S to be the subring of R generated by all a_i and r_i. Since S is a finitely generated ring, and hence noetherian, the previous part of the proof shows that $P\colon C'(S) \to S$ is injective. Let $i\colon S \to R$ denote the injection. Then $x = (C'(i))(y)$, where $y = \sum_i a_i[r_i] + a_0[*] \in C'(S)$. Since $P(y) = P(x) = 0$ we conclude that $y = 0$ and consequently $x = 0$. This completes the proof. ∎

For $p = 2$ we obtain a part of [1, Theorem 1]:

COROLLARY 4. *If $n = 2^l$, $l = 1, 2, \ldots$ then the following are generating relations between the generators $[r] = r^n - r$ of $I_n(R)$:*

(D) $$[rs] = r^n[s] + s[r], \qquad r, s \in R,$$

(C) $$[r + s] = [r] + [s] + N(r, s)[-1], \qquad r, s \in R.$$

Proof. Since $2 = (-1)^n - (-1) \in I_n(R)$, we obtain $I_n(R) = I'_n(R)$. On the other hand, $[0] = [1] + [-1] + N(1, -1)[*]$ in $C'_n(R)$, and this shows that $[-1] = -N(1, -1)[*]$ by Lemma 1(2). It is easy to see that $N(1, -1) = -1$, and hence $[-1] = [*]$. Therefore (C′) = (C) and finally (E) follows from (D) by Lemma 1(1). ∎

References

[1] M. Maciejewski and A. Prószyński, *On n-derivations and relations between elements $r^n - r$ for some n*, Bull. Polish Acad. Sci. Math. 62 (2014), 29–42.
[2] A. Prószyński, *Forms and mappings. I: Generalities*, Fund. Math. 122 (1984), 219–235.
[3] A. Prószyński, *Mappings of Higher Degrees*, WSP, Bydgoszcz, 1987 (in Polish).

Andrzej Prószyński
Kazimierz Wielki University
85-072 Bydgoszcz, Poland
E-mail: apmat@ukw.edu.pl

Received July 23, 2014;
received in final form September 30, 2014 (7978)